Electronic Signatures

E-signature legislation

presented by:

Office of the Secretary of State

Michael Totherow, Chief Information Officer

Russ Savage, Electronic Transactions Liaison

An Electronic Signature...

is just about anything:

- typing ones name
- a digital representation of a hand written name
- a voice recording of an identity and an intent

DEFINITIONS (E-SIGN)

For purposes of this title:

(4) *Electronic Record* —The term "electronic record" means a contract or other record created, generated, sent, communicated, received, or stored by electronic means.

(5) *Electronic Signature* —The term "electronic signature" means an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record.

E-Sign s. 761

(Electronic Signatures in Global and National Commerce Act)

- Based on the Uniform Electronic Transactions Act (UETA)
- Federal law intended for interstate commercial transactions
  - Rushed to pass because of fear UETA uniform adoption would take too long
- Becomes the 'foundation law' for electronic signature laws of the states
- Not technology specific, intentionally Technology Agnostic
- Two parties come together, and as in any contract, they agree to accept a process by which to interact
  - this allows for those electronic processes based on signatory needs 'not to be denied legal effect just because their electronic.'

E-Sign (quoted)

SEC. 101. GENERAL RULE OF VALIDITY. (E-Sign)

(d) RETENTION OF CONTRACTS AND RECORDS.—

(1) ACCURACY AND ACCESSIBILITY.—If a statute, regulation, or other rule of law requires that a contract or other record relating to a transaction in or affecting interstate or foreign commerce be retained, that requirement is met by retaining an electronic record of the information in the contract or other record that—

(A) <u>accurately reflects</u> the information set forth in the contract or other record; and

(B) <u>remains accessible</u> to all persons who are entitled to access by statute, regulation, or rule of law, for the period required by such statute, regulation, or rule of law, in a form that is <u>capable of</u> being <u>accurately reproduced for later reference</u>, whether by transmission, printing, or otherwise.

The E-Sign electronic signature theory

- Parties involved in transaction have most to benefit by ensuring transaction remain effective, so the 'electronic signature process' will be suited to their needs

The E-Sign theory example

- Example:
  - Two parties in a contract of receiving goods agree to accept purchase orders through email. First step is to agree of process and consent to process
    - » Shipping company wants to reduce order overhead, but does not want to ship to phony PO.
    - » Receiving company wants to speed reception, but does not want to be billed incorrectly
    - » Both parties "should" put enough safeguards in signing process to protect their needs in the contractual relationship
    - » E-mail becomes the electronic document purchase order, initials at end are accepted as signature for authorizing PO. That email is accepted as a signed document .
    - » not to be denied legal effect just because it's electronic

Weakness?

That is what E-Sign does -

- They agreed, its documented, it is legal contracting… such that:
  - The laws surrounding the actual "transaction" (the contract law, regulation law, etc) are not altered…
    - » just setting the foundation to complete that transaction electronically is 'enabled'
- a signature shall not be denied legal effect but:
  - Still need to meet the law surrounding the transaction
  - Still need to be able to 'reproduce' the record
  - Still may need to question the entire process

E-Sign Summary

- Technology neutral
- Scope is Interstate commerce / International
  - where no state law, e-sign enables acceptance
  - where state law, e-sign does not pre-empt, as long as state laws are compatible (in theory and technology policy) with E-Sign
- Allows State to address interoperability as party in a transaction
- **Only enables, does not change existing laws surrounding transaction**
- A pretty simple statement - "It's ok to conduct transactions electronically."

Arizona & the Transactions Act

- Arizona Electronic Transactions Act (AETA)
  - followed model UETA
    - » with clarified responsibility for electronic notary
    - » with suggestion for secure electronic signatures/records
  - Does not increase effectiveness of electronic signature
  - Does not require specific technology
- Enables recognition of electronic signatures as a viable signature for Arizona
- Same 'Spirit' as E-Sign
  - based on UETA
  - Technology Neutral
- Scope is commercial transactions within the state

HB 2069 Electronic Transactions Act
44th Legislature
1999-2000 2nd Session
Signed 4/17/2000

AETA (UETA for Az)

Section 9. Attribution And Effect Of Electronic Record And Electronic Signature. (AETA)
 (a) An electronic record or electronic signature is attributable to a person if it was the act of the person. The act of the person may be shown in any manner, including a showing of the **efficacy of any security procedure applied** to determine the person to which the electronic record or electronic signature was attributable.
(b) The effect of an electronic record or electronic signature attributed to a person under subsection (a) is determined from the context and surrounding circumstances at the time of its creation, execution, or adoption, including the parties' agreement, if any, and otherwise as provided by law.

Two similar spirits - however...

- Fundamental component of E-Sign & UETA
  - two parties agree to conduct transactions in an electronic format...

- As a participant in one of these transactions, where State of Arizona is one of those two parties…

  use existing Electronic Signature law 'for the State' to clarify use (namely technology) with and by the State

Arizona Electronic Signature Statute

- ARS 41-132 enacted in 1996, revisited in 1998.
    - Applies to transactions 'with and by state agencies'
    - Technology Neutral
        - » Still anything goes... By Technology "Zoning and Planning" by State
    - Provides criteria to meet as an acceptable technology
        - An electronic signature shall be unique to the person using it,
        - shall be capable of reliable verification, and
        - shall be linked to a record in a manner so that if the record is changed the electronic signature is invalidated
    - Acknowledges digital signature technology as an acceptable technology of electronic signature
- ARS 41-121 enacted in 1998
    - Sets responsibility with the Secretary of State to develop rules along with consultation with GITA, DOA and Treasurer

State... Implementing technology

- **Acceptable Technology**
  - A 'Digital Signature' is an 'Electronic Signature'
    - » it's a subset (not all electronic signatures are created equal)
    - » it's an implementing technology (PKI)
    - » it's an indication of acceptance, not a requirement
      - i.e. it's not the only technology,
        - but a well suited technology process
- **Policy Review an on-going process at the State**
  - Other "signing processes" under review
    - » Shared secret authorization without monetary implication
    - » PGP (Pretty Good Privacy) for initial intent of monetary implication
    - » Non state issued electronic identity as witness to intent of ownership

State Level Summary

- UETA (AETA) enables electronic Signatures within the state
  - Two parties agree to conduct transactions electronically
  - Technology Neutral
  - Scope are transactions in state
- Az Electronic Signature Statute (41-132)
  - Scope with and by the State
    » Technology neutral - but Technology Controlled
        further criteria for State to accept technology processes
    » policy driven - addressed through rule, policy dependent, standard adoption, and procedure implemented
- 'Digital Signatures' are an indication of proven technology, but infrastructure yet to be built

(more on this later)

E-Sign, AETA, 41-132
- scopes narrow

- E-sign is the foundation...
  - Basis of Electronic signatures, including but not limited to interstate transactions
- UETA (AETA) is the in state enabler...
  - covers just about any transaction within the state
- Az Electronic Signature Statute (41-132) is for the state...
  - only for those state government transactions

- Neither requires any person to use or accept electronic signatures
- Neither requires complete commitment to electronic processes
- All acknowledge Electronic Agents
- Electronic signatures are refutable by presumption, just as wet signatures, at the time of creation and integrity over life of document
- Do not alter existing laws surrounding transactions (retention or explicit notification)

Regulatory Constraints

Arizona A.R.S. 41-132 (with/by state agencies)

specific performance requirements that are managed by the Secretary of State

E-SIGN

"…Federal regulatory agency or State regulatory agency may... specify performance standards to assure accuracy, record integrity, and accessibility of records that are required to be retained."

Responsibility falls upon the Secretary of State, as the Policy Authority,

to develop the performance standards of the State

Legal Roadmap

STATUTE §41-126, §41-132
- Electronic Signatures (ES) EQUATES Wet Signature (handwritten)
- SOS responsible, in consultation with GITA, DOA and Treasurer, to develop rules
- Digital Signature (DS) is an acceptable technology of ES

Rules (Title 2, Chapter 12, Article 5)
Outline actions by SOS to enable Statute
- Policy Authority (PA)
- Acceptable Technologies
  - DS
  - Approved List of Certificate Authorities

Policy Authority (SOS)

Carat Guidelines (v1.0)
Definition of PA and its responsibilities towards DS

PA Practices
Outline actions to enable entity in responsibilities

AESI Guidelines
- Requirements
- Outline
- Responsibilities
- Reporting

GITA ES/DS Technology Standard
Specifies technologies acceptable for use
- DS
- PKI framework

SLAPR E-Records Archiving
Specifies technologies acceptable for use
- Evolving e-records management
- Acceptable practices

Certificate Policy (CP)
CP is accepted by PA
- Draft
- Public Review
- CP assigned OID
- CP revision (Versioning required)
CP Identifies
- Parties using (ALCA & AESI Projects)
- Applicability (AESI Projects)
- Policies of
- Authentication
- Issuance
- Obligation
- Liability
- Content

Approved List of Certificate Authorities
As Cas approved, they are added to list
- SAS 70
- Insurance Verification
- Agree to CP

AESI PKI approved processes
As projects are approved, they are added to list
- Application for signing process (Description)
- SOS acknowledges project (Added to List)
- Agency picks CP (To identify AESI)
- Agency contracts with CA (To build AESI)
- Agency reports to SOS on project (Informative)

Policy Authority

- Accepts and approves technology
  - Follows American Bar Association "Guidelines for Public Key Infrastructure"
    - Defines Roles
    - Defines Responsibilities
    - Defines Relationships
    - Defines Liability
  - Applies Four Corner Model to new technologies
    - Approves and Maintains Certificate Policies

The Four Corner Model

How do you know the person is who he says he is?
    Verified by reputable source -
    Chain of trust (chain of reputable sources) -
Authenticating the person associated with a record
    is not the same as showing intent to sign or establishing integrity of a signing

To build an electronic signature infrastructure, the state has:

- Policy Authority establishing the planning and zoning for the infrastructure (Office of the Secretary of State)

- Certification Authority registering the subscriber & issuing digital certificates (CA approved by Secretary of State).

- Agency contracting with the CA for services.

- Subscriber getting a certificate to have a digital signature.

- Relying Party verifies the digital signature received from the subscriber.

The Roles in Electronic Signature Use
(State of Arizona's infrastructure model)
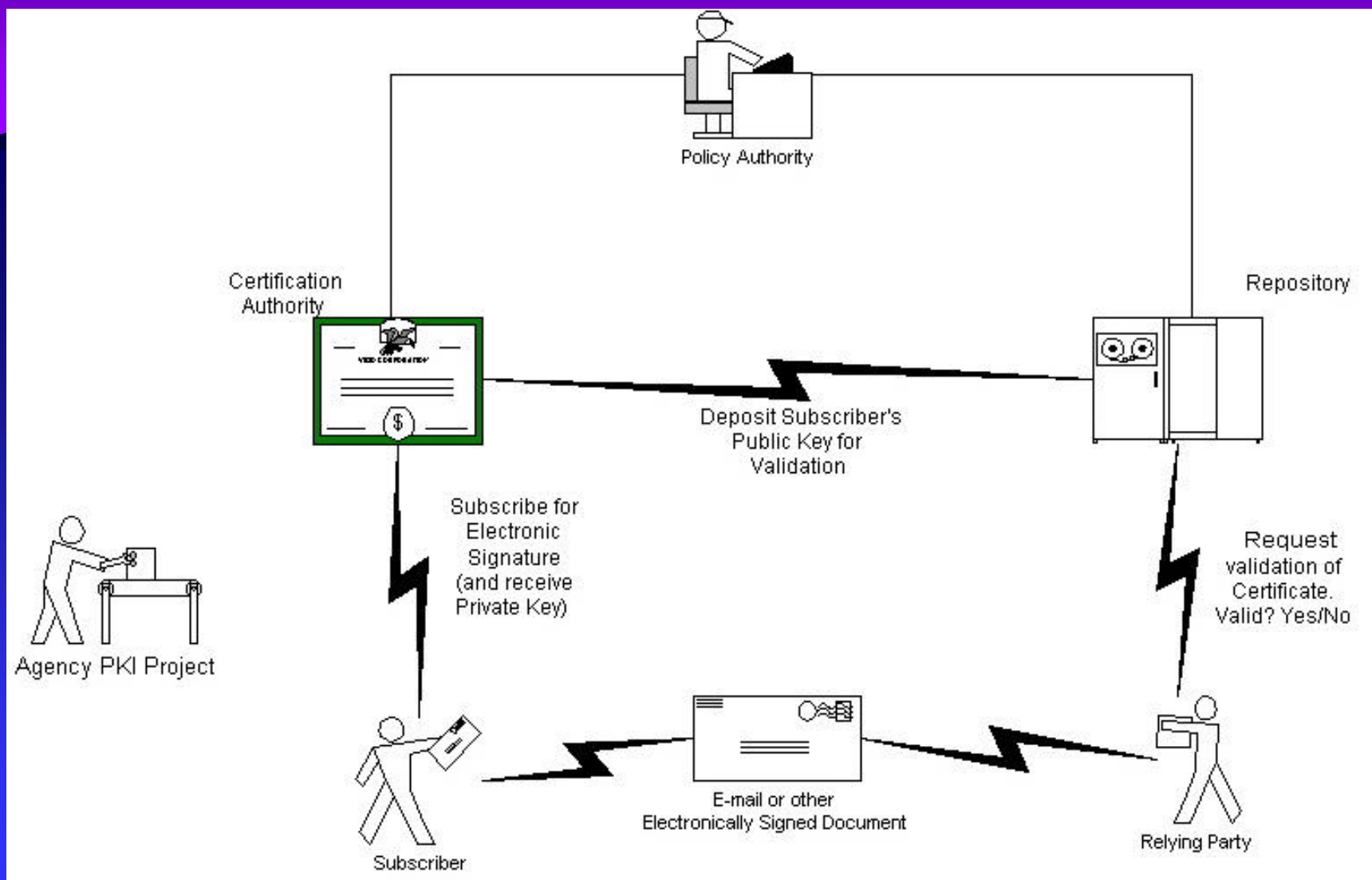
PKI Roles & Responsibilities

- Subscriber
  - "subject"/holder of the signature
  - Subscriber Agreement (policy, contract)
  - keep signature private (sole control)
- Relying Party
  - party whose application requires signature validation
  - Relying Party agreement (policy, contract)

PKI Roles & Responsibilities

- Certification Authority
  - Operates mechanisms of PKI
  - Registration Authority
    - Verify identity of applicants to become subscribers (in-person)
  - Issuance
    - Manufacture and issue electronic signatures
    - Ensure subscriber possession of electronic signature
  - Frequent Compliance Audits
  - Liability / Contract intensive function
- Repository
  - Maintain electronic signatures integrity
  - secure facilities, with public access

Certificate Policy is the zoning for construction

- Outlines the roles
- Describes the responsibilities and liabilities
- Limits the scope of application
- Determines location within Infrastructure
- Establishes the trust amongst the community

The Structure of Electronic Signatures

Zoning for Infrastructure is Summarized in CP
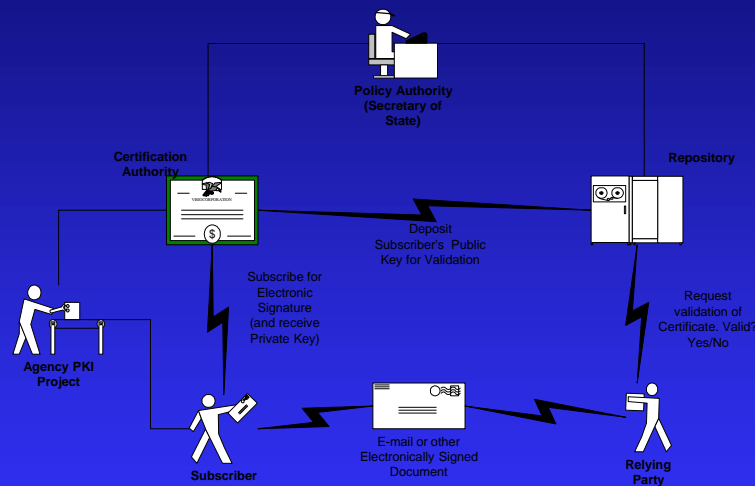
Certificate Policy: "Signing Process"
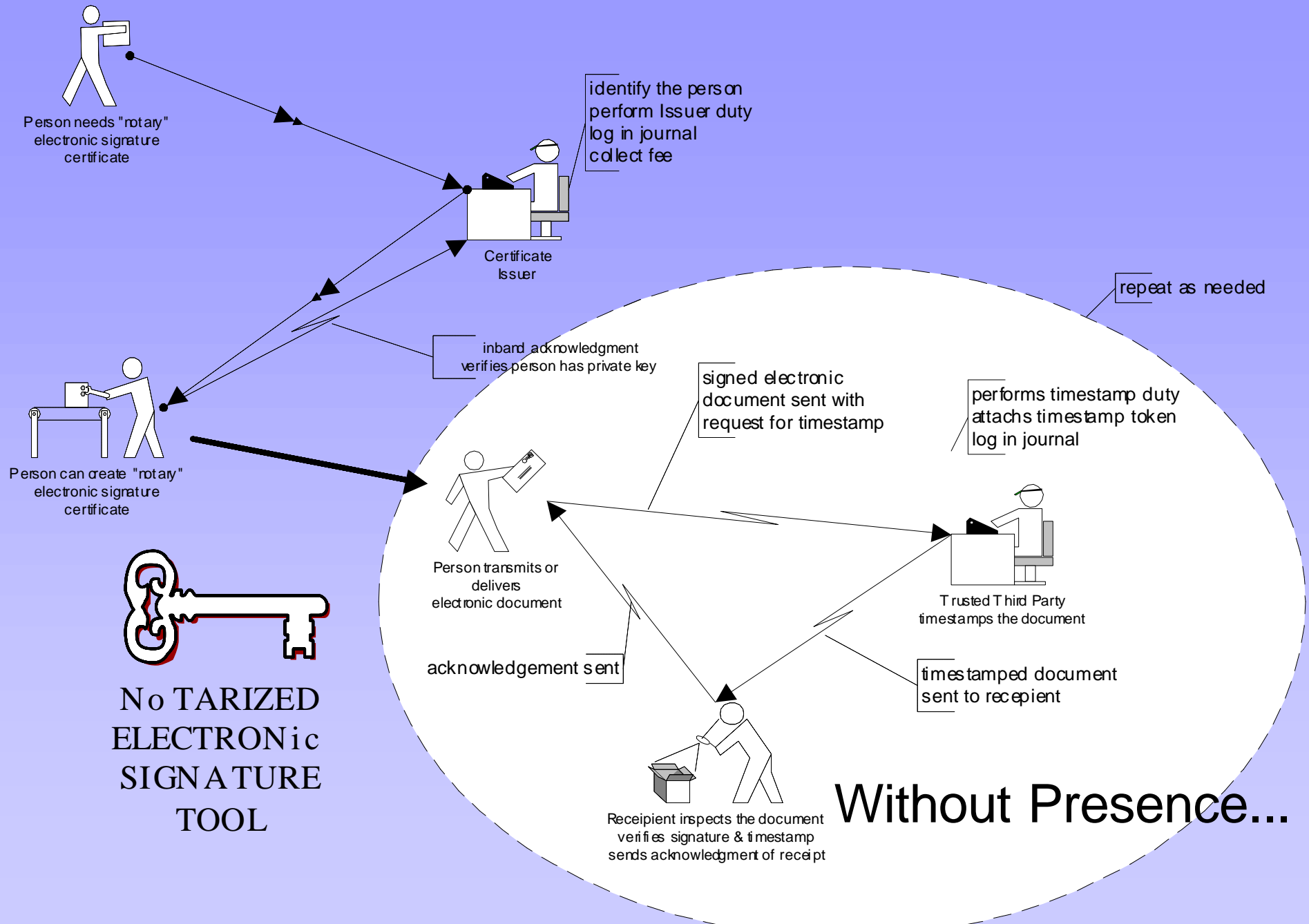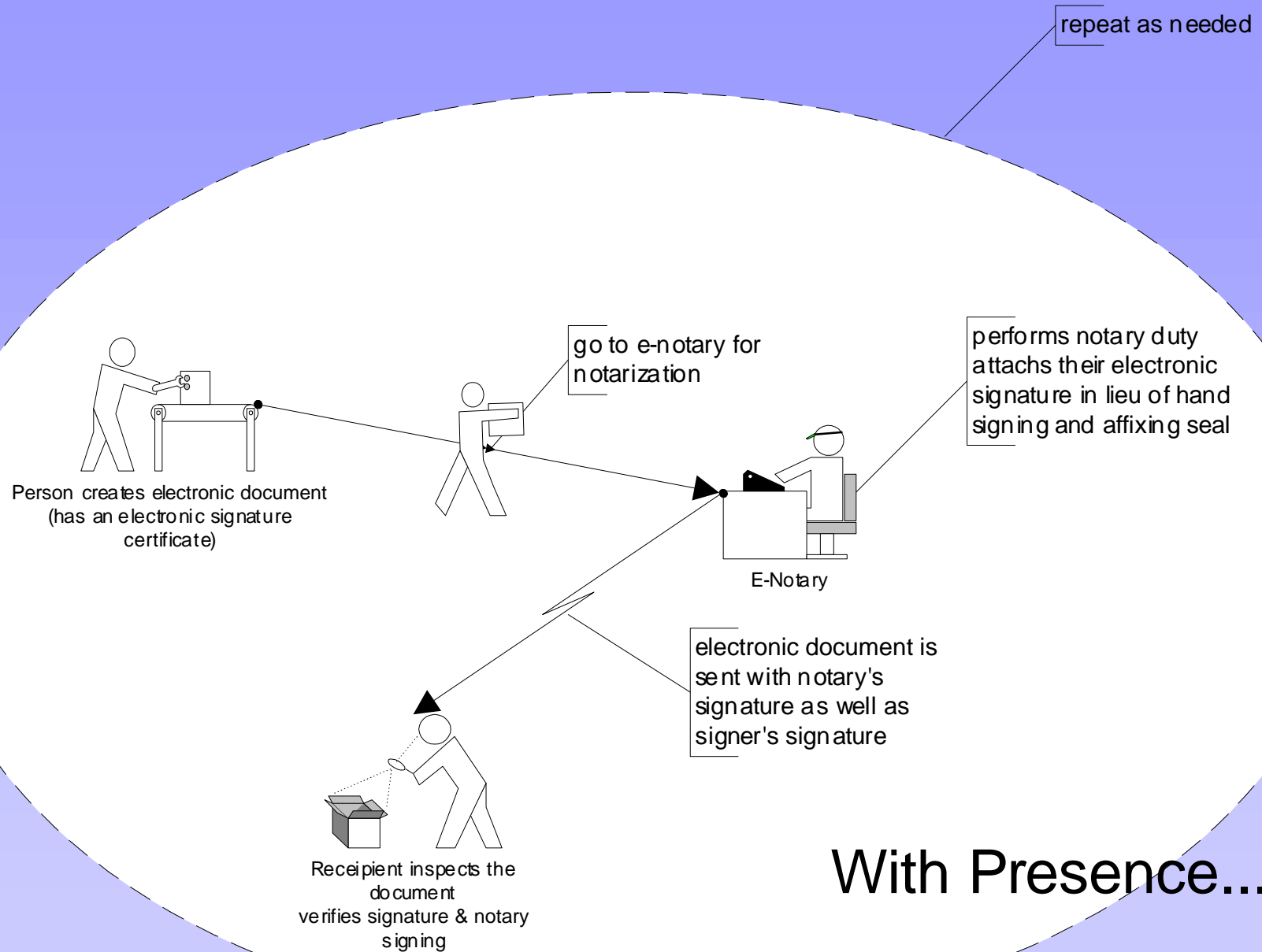
the 'Contract of Process'

Example of applied Infrastructure

- E-Notary
  - Uses CP set by Policy Authority
  - Uses Digital Signature Technology
  - Uses foundation of E-Sign/UETA
    - Signature of individual could be anything
      - typed name!
  - E-Notary law agnostic, but uses existing legal structure
  - Gives state ability to specify technology as controlled by the state

Electronic Signature "Notary" Process

Person needs "notary" electronic signature certificate

identify the person
perform Issuer duty
log in journal
collect fee

Certificate Issuer

inband acknowledgment
verifies person has private key

Person can create "notary" electronic signature certificate

NoTARIZED ELECTRONic SIGNATURE TOOL

repeat as needed

signed electronic document sent with request for timestamp

performs timestamp duty
attachs timestamp token
log in journal

Person transmits or delivers electronic document

Trusted Third Party timestamps the document

acknowledgement sent

timestamped document sent to recepient

Receipient inspects the document
verifies signature & timestamp
sends acknowledgment of receipt

Without Presence...

Notary Electronic Signature Process

repeat as needed

go to e-notary for notarization

performs notary duty attachs their electronic signature in lieu of hand signing and affixing seal

Person creates electronic document (has an electronic signature certificate)

E-Notary

electronic document is sent with notary's signature as well as signer's signature

Receipient inspects the document verifies signature & notary signing

With Presence...

Zoning and planning the Infrastructure

– Electronic Signature

  • Secretary of State (scope, use, feasibility, assistance)

– Project oversight

  • Government Information Technology Agency (PIJ)

– Payments for those on line transactions

  • Treasurer's Office (authority for credit card acceptance)

  • General Accounting Office (transaction accounting)

– Sufficient evidence of transactions

  • Attorney General's Office

– Records retention, now e-records retention

  • State Library and Archives

Points of Interest

Arizona Secretary of State

– http://www.sosaz.com/pa

E-Sign summary

– http://thomas.loc.gov/cgi-bin/bdquery/z?d106:s.00761:

AETA

– http://www.azleg.state.az.us/ars/44/title44.htm

Electronic Signatures Statute (41-132) & Electronic Notarization (41-351)

– http://www.azleg.state.az.us/ars/41/title41.htm

UETA watch

– http://www.uetaonline.com/

Russ Savage

rsavage@sos.state.az.us

Michael Totherow

mtotherow@sos.state.az.us